

<input type="text"/>	<input type="text" value="Search"/> KY GOT: <input type="text" value="?"/> <input type="button" value="x"/>	Other Search Options
		<h1>Security Awareness</h1> <p>January 2003</p>

Microsoft Outlook Email Security Update	Configuring ZoneAlarm Firewall	Cyber Bytes
Password Tips	Securing Your Workstation	Microsoft Information
Security Tips for Home Computer Users	HIPAA Security	Useful URLs

Foreword

In an effort to emphasize the importance of information security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide the Security Awareness Newsletters. It is hoped these newsletters will be a valuable resource, providing practical tips, security solutions, and job-saving techniques.

Also, as a friendly reminder, GOT staff are encouraged to familiarize themselves with all security policies, manuals, and procedures which can be found at [GOT Policies and Procedures](#).

[Back to Top](#)

Microsoft Outlook Email Security Update



Over the years, numerous security lapses and holes have been discovered in Outlook, prompting Microsoft to release various patches to fix these problems. Recently Microsoft has released the [Outlook Email Security Update](#), available for Outlook 98 or 2000. (Please note that this update is not available for Outlook 97 and comes built-in to Outlook 2002). While this update offers increased protection, it may drastically alter the way you are used to seeing Outlook operate.

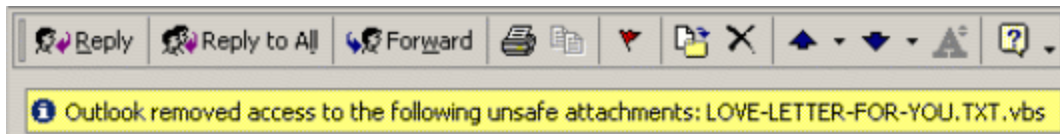
Be aware that once you install the update, you CANNOT uninstall it -- you will have to reinstall Office to remove it. Before installing the update it is probably a good idea to read [\(Q262618\) OL98: Known Issues with the Outlook E-Mail Security Update](#) (for Outlook 98) or [\(Q262634\) OL2000: Known Issues with the Outlook E-Mail Security Update](#) (for Outlook 2000).

Below is a list of some of the functions that the Outlook Email Security Update provides:

Unsafe File Notification

Email attachments that contain files that Microsoft classifies as "unsafe" are blocked. Unsafe files include batch files (.bat), Windows Installer Packages (.msi), DOS Applications (.com), Photo CD Images (.pcd), Registry Entries (.reg), Applications (.exe), Screen Savers (.scr), Windows Help Files (.hlp), Internet Shortcuts (.url), and Program Shortcuts (.lnk). These files can still be sent as attachments; however, anyone with a version of Outlook that has this blocking feature will not be able to open or access these files.

Below is an example of the message you will see if you receive an email where a file has been blocked.



Object Model Guard

Viruses, worms, and other malicious code are often spread by accessing a user's address book and then sending infected emails to those listed in the user's address book. To prevent programs from accessing your address book or sending email without your approval, Microsoft has included the Object Model Guard in their Outlook Email Security Update. If a program tries to access your address book, Outlook will warn you and then give you the option to proceed or not.

Please note that while most malicious code requires that the user open an attachment to activate it, many now run merely if the user previews the email in the Preview Pane. To prevent this, users should turn off the Preview Pane in Outlook.

Security Zone

The Outlook Email Security Update automatically changes the Security Zone used by Outlook to "Restricted" which will protect your computer from unsafe software when downloading or running programs from the Internet.

For more information about the Outlook Email Security Update, as well as where to download it, click [here](#).

If you should need assistance in installing the update, please contact your network administrator or other technical resources.

[Back to Top](#)

Password Tips



Creating and maintaining a secure password is one of the most important things you can do to protect your data and files, as well as the network infrastructure. In order to ensure that the State's networks remain secure and free from compromise, the Governor's Office for Technology's password policy mandates that all passwords must be at least 8 characters in length (11 if the account has privilege access, such as a systems administrator account). Passwords must be comprised of upper/lower case letters, numbers, and at least one special character (if the application allows) and must not include dictionary words, phrases or names. Sure, all of this sounds like a good idea, but how do you remember such a complex, cryptic password? Below are a few tips to help you create policy-compliant passwords that you can remember:

- **Combine first letters from a phrase.** Lines from poems or songs often work well. For example, "Four score and seven years ago our fathers" could be written as 4s&7YaOf.
- **Remove vowels and consonants from words.** Take a short phrase and take out all of the vowels or consonants. You will need to add numbers and special characters to get a good password. For example, "Jack and Jill went up the hill" would be translated to JaJ^wuTh7
- **Create pseudo words.** Link one or two consonants followed by one or two vowels and repeat the pattern. The idea is to come up with a "word" that sticks with you but that does not appear in any dictionary. You will also have to mix in some numbers and special characters. For example, prAu*cd9

[Back to Top](#)

Security Tips for Home Computer Users



So who would want to break into your home computer? Hackers may care less about who you are than gaining control of your computer to launch attacks against other systems. Once intruders gain access to your system, they can do a variety of malicious acts such as sending forged email from your computer or examining personal information such as your financial statements. In addition, if you use your home computer to access email and other applications on your office PC, you may be placing the State's networks in jeopardy if you don't have adequate security measures in place. Below is a list of tips provided by the [NIPC](#) (National Infrastructure Protection Center) to thwart such compromises:

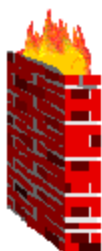
- **Use strong passwords.** Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts. ***GOT recommends using passwords that are at least 8 characters in length and contain a combination of upper/lower case letters, numbers, and at least one special character.***
- **Make regular backups of critical data.** Backups must be made at least once each day and at least once a month the backup media should be verified.
- **Use virus protection software.** That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically. ***If you are a GOT employee or your agency participates in the McAfee Active Virus Defense Program, you may be eligible to receive free McAfee VirusScan software for your home computer. Contact Shawn Thomas for more information.***
- **Use a personal firewall as a gatekeeper between your computer and the Internet.** Firewalls are usually software products. They are essential for those who keep their computers online through the popular DSL and cable modem connections but they are also valuable for those who still dial in. ZoneAlarm is free for home use and can be downloaded at the [Zone Labs](#) website. More information on ZoneAlarm can be found in the following article "Configuring ZoneAlarm for Home Use."
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Do not open email attachments from strangers**, regardless of how enticing the subject line or attachment may be. **Be suspicious of any unexpected e-mail attachment from someone you do know** because it may have been sent without that person's knowledge from an infected machine.
- **Regularly download security patches from your software vendors.**
- **Follow the same security procedures at home as you do for work.**

Remember information security is everyone's responsibility - at home

and at work!

[Back to Top](#)

Configuring ZoneAlarm for Home Use



In the preceding article, we outlined the importance of installing a personal firewall such as ZoneAlarm on your home computer to keep hackers at bay, especially for those users who have "always on" DSL, ISDN, or cable modem connections to the Internet. Since most software tools do not work effectively unless configured correctly, we want to provide you with some tips to setting up ZoneAlarm on your home PC.

The first time you open ZoneAlarm, a simple installation and setup wizard will help you determine how you'll use the program. The questions it asks are based on the type of connection you specify.

- **Do you want ZoneAlarm to notify you when it blocks Internet traffic or do you want it to protect in silence?** If you're easily annoyed by pop-ups, choose to be protected in silence. You will still be asked to verify programs.
- **Do you want ZoneAlarm to configure your browser's security settings right away or the first time you launch your browser?** For most users, it is recommended to do this right away. Advanced users will want to customize access and server permissions. Most novice users should stay away from the Advanced options.

Now that you're finished with setup, you can customize even more settings:

Overview

Quickly view how much traffic ZoneAlarm has blocked, which programs have attempted to go online, and how many email attachments are quarantined.

- Go to the Product Info tab to get version, licensing, and registration information as well as product updates and help.
- The Preferences tab contains ZoneAlarm's display properties, lets you decide how to communicate with Zone Labs, and determines how you want to check for updates.

Firewall

Firewall settings are broken into two categories: Internet Zone Security and Trusted Zone Security.

- The Internet Zone Security option includes all computers on the Web. Putting this setting on Low turns off your firewall protection. Medium is

recommended for limited Internet use. Other users can see your computer but can't share its resources. High is recommended for always-on Internet users.

- Trusted Zone Security lets you share files with other "trusted" users. Low turns off the firewall. Medium lets you share files. High hides your machine and keeps it operating under hackers' radar.
- Use the Advanced button to tweak your security settings by blocking specific types of incoming and outgoing traffic.
- Go to the Zones tab to add computers to your Trusted Zone.

Program control

It's recommended that you keep Program Control on the Medium setting so that each program requests permission to access the Net. Here's how to use the other options in this field. You can also access the Program Wizard if you want to change any of the original options you chose during setup.

Automatic Lock shuts off Internet access after a period of inactivity. Press the Custom button to specify what amount of time determines "inactivity" or choose to have it activate when the screen saver comes on. You can also determine if you want to block all Internet traffic or grant permission to pass-lock programs.

- Go to the Programs tab and left-click one of the symbols next to a program's name to change its access: Allow, Block, or Ask.

Alerts and logs

Say whether or not you want to get alert pop-up messages for things that are not programs. The Log Viewer lets you look over all the alerts you've received.

Email protection

Turn MailSafe on and off. This feature spots questionable email attachments that may contain viruses and puts them in quarantine. In general, keep it on.

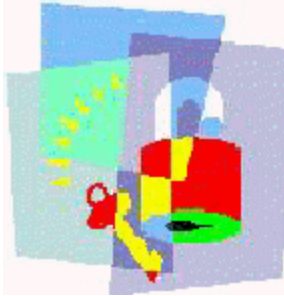
It's easy to minimize ZoneAlarm's screen. If you want to turn off the program for any reason, right-click the icon in your system tray and choose Shutdown ZoneAlarm.

If you would like additional information on using ZoneAlarm, there is also a [Zone Labs User Community](#) that lets you discuss issues with other ZoneAlarm Users, as well as an online [ZoneAlarm Manual](#).

Note: Currently the Governor's Office for Technology does not have an enterprise standard for personal firewall software. Please note that GOT in no way endorses the use of ZoneAlarm, especially for use on state government-owned computers. This article simply attempts to provide a low cost solution for home computer users to protect their workstations.

[Back to Top](#)

Securing Your Workstation when You're Away



Did you know that leaving your workstation unlocked when you are away from your office is an open invitation for someone to access your data and files. Someone could possibly use your machine to send unauthorized emails from your account or access sensitive information, not to mention place the entire network at risk. Even if you are just going to be away from your desk for a few minutes, it is a good idea to lock your workstation by pressing **CTRL+ALT+DEL** and then pressing **LOCK COMPUTER**. It is also wise to use password-protected screensavers to prevent unauthorized access to your PC. And always power down (turn off) your computer before leaving for the day. Certain computers may need to remain on continuously. For these exceptions, a [GOT-F085 Security Exception Request](#) must be completed to request exception to the policy. By following these simple procedures, you may save yourself, as well as the network support staff, a lot of headaches.

[Back to Top](#)

What Does HIPAA Security Mean to You?

No, we are not referring to the large, chiefly aquatic mammal, indigenous to Africa. We're talking about the Health Insurance Portability and Accountability Act (HIPAA), which was enacted in 1996 to standardize electronic patient health, administrative and financial data. HIPAA is not a simple subject to cover, affecting many state government agencies (not to mention numerous private entities) including Medicaid, Health Services, Insurance, Universities, and various other agencies. HIPAA covers a large area ranging from health care reform to the Administrative Simplification provisions that establish national standards for electronic health care transactions. An important aspect of HIPAA includes protecting the confidentiality and security of health care data by introducing and enforcing standards. HIPAA has published security standards which include well known industry standards and best practices many of which the Governor's Office for Technology currently recommends, supports, and implements such as:

- Implementing and enforcing security and confidentiality policies
- Designating information security officers
- Implementing security awareness education and training programs
- Applying access controls, audit trails, physical security and disaster recovery, and many more.

As of January 2003, the HIPAA Security Regulations have not been released in final form. However, the proposed Standard has been available since August 1998, and its general provisions are not expected to change significantly when the final rule is released soon. To

learn more about the HIPAA security standards, check out the [Security and Electronic Signature Standards](#) located on the [U.S. Department for Health & Human Services](#) website.

GOT also has a contact for HIPAA, Kathy Frye, who works with the Office of Consulting and Project Management. If you would like more information you can contact Kathy at 502.573.7017, ext. 111 or by [email](#).

[Back to Top](#)

Cyber Bytes



U.S. Arrests Queens, New York Man on Computer Fraud Charges

JUJU JIANG, 24, of Flushing, Queens, New York, was arrested on charges of computer fraud for attempting to gain access to the accounts of numerous subscribers of GoToMyPC.com, a computer services company that provides subscribers with remote computer access, and successfully taking control of one of those accounts.

GoToMyPC is a company that offers individuals the ability to remotely access their personal computers from any computer connected to the Internet. According to the complaint, JIANG obtained these users' passwords and user names by installing computer software for this purpose at a Kinko's located on Seventh Avenue in Manhattan. JIANG then used these passwords and usernames in attempts to gain access to those subscribers' personal computers in order to obtain credit card and other information stored on those computers. If convicted, JIANG faces a maximum sentence of 5 years in prison and a \$250,000 fine.

Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing "Logic Bomb" on Company Computers

Roger Duronio, 60, of Bogota, N.J., a disgruntled computer systems administrator for UBS PaineWebber was charged with using a "logic bomb" to cause more than \$3 million in damage to the company's computer network, and with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb, U.S. Attorney Christopher J. Christie announced.

The Indictment alleges that, from about November 2001 to February, Duronio constructed the logic bomb computer program. On March 4, as planned, Duronio's program activated and began deleting files on over 1,000 of UBS PaineWebber's computers. It cost PaineWebber more than \$3 million to assess and repair the damage, according to the Indictment. As one of the company's computer systems administrators, Duronio had responsibility for, and access to, the entire UBS PaineWebber computer network, according to the Indictment. He also had access to the network from his home computer via secure Internet access.

Duronio is charged in Count One of the Indictment with securities fraud, which carries a maximum penalty of 10 years in federal prison and a \$1 million fine. He is charged in Count Two with Fraud and Related Activity In Connection with Computers. That charge carries a maximum prison sentence of 10 years and a fine of \$250,000 or, alternatively, two times the gain made by the defendant or the loss suffered by the victim.

Federal Website Hacker Faces 10 Years in Prison

William Douglas Word of Pelham, Alabama, has pleaded guilty to 17 counts of defacing government websites and faces up to ten years in prison. He was also charged with one count of possessing counterfeit or unauthorized credit cards.

Word was charged with defacing sites of NASA, Defense Department agencies, Interior Department and the International Trade Commission, among others, in late 1999. More information on this article can be found at [Government Computer News](#).

The Real Cost of Spam

A study released in early January estimates the annual cost of Spam to be \$8.9 billion for U.S. companies, \$2.5 billion for European businesses, and another \$500 million for U.S. and European service providers.

Taking into account that it takes 4.4 seconds on average to deal with these unwanted emails, the emails add up to \$4 billion each year in lost productivity for U.S. companies.

Another \$3.7 billion comes from companies having to buy more powerful servers and more bandwidth as well as divert staff time. The rest is attributable to companies providing help-desk support to annoyed users.

[Back to Top](#)

Microsoft Information

Microsoft Issues Patches for Multiple Vulnerabilities

- Microsoft recently recommended users apply patches for multiple new vulnerabilities. The most serious flaw is rated critical and could allow an attacker to gain control over another user's system. The "Flaw in Microsoft VM Could Enable System Compromise" consists of eight vulnerabilities and affects Microsoft Virtual Machine (VM) for the Win32 operating environment. According to Microsoft, the flawed version exists in most versions of Windows, as well as in most versions of Internet Explorer. [A patch is available via the Windows Update site.](#)
- The "Flaw in SMB Signing Could Enable Group Policy to be Modified" vulnerability is rated moderate and affects Windows XP/2000. According to Microsoft, Server Message Block (SMB) is a file-sharing protocol natively supported by all versions of Windows. A

flaw in the implementation of SMB Signing in Windows XP/2000 could enable an attacker to silently downgrade the SMB Signing settings on an affected system. This could permit SMB session tampering or allow an attacker to run code of his choice on the system. Microsoft recommends that administrators using Windows 2000/XP Gold systems configured to use SMB Signing install the patch immediately. [A patch is available via the Windows Update site.](#)

- The "Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation" vulnerability affects Windows NT 4.0/XP/2000 and is rated important. A Windows timer message can be used to cause a process to execute a timer callback function. According to Microsoft, a security vulnerability results because it's possible for one process in the interactive desktop to use a WM_TIMER message to cause another process to execute a callback function at the address of its choice, even if the second process did not set a timer. Microsoft recommends installing the patch at the earliest opportunity. [A patch is available via the Windows Update site.](#)

Microsoft Revises Vulnerability Ranking Again

Microsoft is upgrading the severity level of a vulnerability advisory regarding Internet Explorer (IE). Microsoft is changing the rating of a vulnerability in the way some versions of IE run the Portable Network Graphics (.PNG) image graphic from important to critical. The exploit delivers malformed code that instructs the computer to continually re-read a piece of the image file. This can cause a memory buffer overflow, which could enable an outsider to run code with the rights of the legitimate user. Microsoft is updating the advisory to "critical," according to a spokesperson for the company's public relations firm. Microsoft released an advisory on Dec. 4 stating that a vulnerability to an object caching vulnerability in IE 5.5 and 6.0 was moderate. The company was forced to upgrade the warning to severe after being given information about how the flaw could be exploited. [Microsoft recommends using original patch or a subsequent patch released on Dec. 4.](#)

Microsoft Releases Update to Microsoft Security Baseline Analyzer (MSBA)

Microsoft released a minor update to its Microsoft Security Baseline Analyzer (MSBA), which scans for common security misconfigurations and missing security updates in Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server 4.0, Internet Information Services 5.0, SQL Server 7.0 and SQL Server 2000. MSBA also scans Exchange 5.5 and 2000, Internet Explorer 5.01 and later and Windows Media Player 6.4 and later for missing security updates. The product runs on Windows 2000 and Windows XP. The 1.0 version came out early this year. New features in the 1.1 version include the Exchange and Windows Media Player security update detection, full support for HFNetChk version 3.81 in the command-line interface, support for Software Update Services during security update scans, compatibility with the SMS 2.0 Software Update Services Feature Pack and detection of multiple SQL Server instances. More information and a

download URL may be found at the [Microsoft website](#).

Some of the articles featured here were gathered from information provided by the Security Wire Digest.

[Back to Top](#)

Useful URLs

www.cert.org

The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com

Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com

Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through e-mail, voice message, fax, or SMS (Small Message Service) on wireless phones. SIA provides all known information available about vulnerabilities, their causes, and severities creating actionable information to bolster computers from attack.

<http://www.zdnet.com/>

ZDNet operates a worldwide network of Web sites for people who want to buy, use, and learn about technology. Winner of the Computer Press Association's "Best Overall Site" award for two consecutive years, ZDNet provides an invaluable perspective and resources for technology decision makers to gain an edge in business.

<http://www.searchsecurity.com/>

SearchSecurity.com is the home of TechTarget, offering the most targeted media for enterprise IT professionals, including industry-specific web sites, more than 100 e-mail newsletter titles, print media, exclusive, invitation-only conferences, live online events and list rentals.

[Back to Top](#)

Sources: NIPC, Security Wire Digest, TechTV.com, Cybercrime.gov, Information Week, Government Computer News, Security Focus Online, University of Illinois Computing & Communication Services Office

For other Kentucky
Government sites visit:
 kentucky.gov

[Feedback](#) | [Privacy](#) | [Disclaimer](#) | [Individuals with Disabilities](#)

Copyright © 2003 Commonwealth of Kentucky.
All rights reserved.

